Soft Computing Fusion with Applications

www.scfa.reapress.com

Soft. Comput. Fusion. Appl. Vol. 1, No. 3 (2024) 134–143.

Paper Type: Original Article

Seamless Connectivity: Leveraging IoT for Autonomous Vehicle Networks in Smart Cities

Aditya Raj*

School of Computer Science Engineering, KIIT University, Bhubaneswar, India; 22052873@kiit.ac.in.

Citation:

Received: 27 January 2024 *Revised: 06 June 2024* *Accepted: 10 July 2024*	Raj, A. (2024). Seamless connectivity: Leveraging IoT for autonomous vehicle networks in smart cities. *Soft computing fusion with applications, 1*(3), 134-143.

Abstract

Integrating Autonomous Vehicles (AVs) with the Internet of Things (IoT) revolutionizes urban transportation in smart cities. This paper investigates how IoT contributes to the networking of AVs and improves transportation efficiency, safety, and sustainability. By utilizing Vehicle-to-everything (V2X) communication, IoT facilitates immediate data sharing among vehicles, infrastructure, and pedestrians, fostering adaptive traffic management and enhanced urban planning. The key elements discussed include sensor integration, data analytics, and communication protocols that power these networks. Case studies from various smart cities showcase effective implementations of IoT-enabled AV networks, emphasizing advantages such as decreased congestion, heightened safety, and reduced emissions. However, despite these advances, issues such as cybersecurity, interoperability, and scalability remain, requiring ongoing research and development. This study highlights the importance of tackling these challenges to fully realize the potential of IoT in the networking of AVs. Ultimately, our findings stress the vital importance of IoT in transforming urban mobility, leading to smarter, more interconnected cities that focus on efficiency and sustainability.

Keywords: Autonomous vehicles, Internet of things, Smart cities, Vehicle-to-everything communication, Urban mobility.

1 | Introduction

Vehicular Sensor Networks (VSN) provide connected sensor devices to collect data and use it to provide safer and more fluid traffic on the roads [1]. Contemporary vehicles have been fitted with various sensing devices such as actuators, Global Positioning Systems (GPS) [2] devices, and micro-embedded computers [3]. Consequently, many vehicles can collect and process data. Moreover, the vehicles can communicate with other vehicles or with road-side infrastructure using communication protocols such as Hypertext Transfer Protocol (HTTP) [4], Simple Mail Transfer Protocol (SMTP) [5], Wireless Application Protocol (WAP) [6], and Next-Generation Telematics Protocol (NGTP) [7].

Corresponding Author: 22052873@kiit.ac.in

https://doi.org/10.22105/scfa.v1i3.44

Licensee System Analytics. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0).

Fig. 1. Example of a traffic congestion.

The communication paradigm lets vehicles receive and securely send the processed data to other vehicles or infrastructure units. As a result, vehicular technology such as remote engine shutdown and remote vehicle diagnostics, anti-collision systems, and road sign notifications, among others, have been developed. These technologies utilize VSNs to enhance road users' safety, convenience, and comfort. The data collected by sensors used in VSNs is confidential and can be used to harm innocent users. Security in the VSN paradigm is, therefore, critical. Securing VSNs is securing the sensor network against malicious attacks using modern technologies. Advances in the Internet of Things (IoT) have provided opportunities for tremendous technological growth in VSNs. Therefore, to analyze the security aspect of VSNs, we must briefly discuss one of the VSN's main future enablers, IoT, and its security features. Subsequently, providing the reader with a clear understanding of the importance of securing the VSN paradigm.

IoT is a unique system attaining rapid recognition in the world of contemporary wireless telecommunication. IoT will consist of billions of devices, people, objects, and services that seamlessly communicate and exchange information about themselves and their environment. As stated by [8], the next generation of computing will be completely different from the common desktop interactions. The basis of this concept is the rich and ever-growing presence of smart objects and things all around us. Most of these objects will be in the network in one form or another. Such objects include tags, Radio-Frequency Identification (RFID) [9] devices, switches, and so on. With their unique addresses, these "Things" can interact, exchange information, and work together to attain a common goal. For instance, recently, a few cloud-based systems used to provide a plethora of services have been put forward. The cloud-based service connects different devices and provides services to the users [10]. For example, the authors propose Intelligent Transportation Systems (ITS)-cloud [11], a new vehicular cloud-based paradigm used to improve vehicle-to-vehicle communication and security. ITS-cloud provides many services through correspondence, cloud backup, business, and research applications. Security in IoT devices is of utmost importance. Devices should be equipped with built-in security barriers to impediment and isolation, and countermeasures should be recognized, diagnosed, and executed against successful infringements. Currently, VSNs are being employed in a smart city setting.

Smart city implementation can be perceived as mitigating the challenges sparked by the exponential population growth in urban developments. A forecast done by the United Nations Population fund suggests that 60% of the world's population will inhabit urban environments in 10 years. Consequently, 27 megacities with a population of about 10 million are expected to exist in the next 10 years. A vehicular traffic-related problem such as traffic congestion is one of the biggest challenges most significant cities face. Vehicles in the 75 largest urban areas in the US have recently accumulated about 3.6 billion hours of delay. Moreover, this

led to 5.7 billion gallons of wasted fuel, translating to $67.5 billion in production loss [12]. As a result, various ways of reducing the cost of transportation are being invented. Utilizing VSNs in the transport sector will save a lot of money by providing a secure data collection and communication system to enable the deployment of services such as efficient traffic routing and accident prevention. Nevertheless, high-security precautions must be employed in VSNs' paradigms while providing much-needed services.

Fig. 2 illustrates the framework of a smart traffic controlling and monitoring system, highlighting its key components and functionalities. This system integrates various technologies, including IoT sensors, traffic cameras, and communication networks, to gather real-time data on vehicle flow, speed, and congestion levels. The data collected is analyzed using advanced algorithms to optimize traffic signals, enabling adaptive signal control that adjusts timing based on current traffic conditions. This dynamic approach reduces wait times and improves overall traffic efficiency. Additionally, the system incorporates predictive analytics to forecast traffic patterns and potential congestion points, allowing for proactive management strategies. The visual representation emphasizes the interconnected nature of components within the smart traffic system, showcasing how data from multiple sources feeds into a centralized management platform. This holistic view demonstrates the potential for enhanced coordination between vehicles, infrastructure, and traffic management agencies, ultimately contributing to safer and more efficient urban transportation.

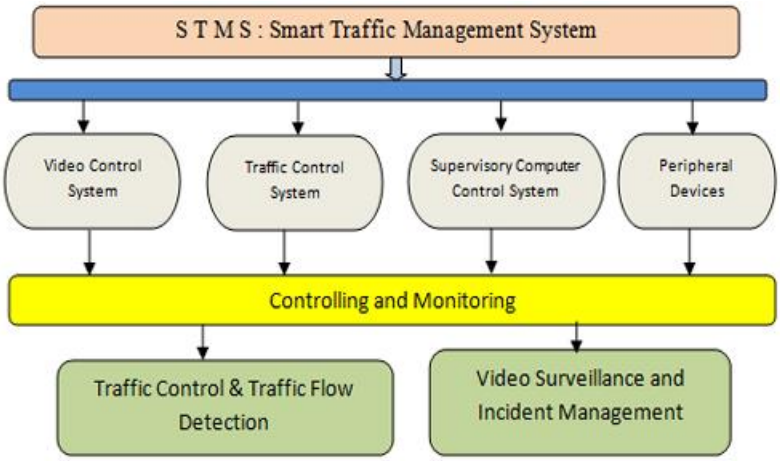
S T M S : Smart Traffic Management System
Video Control System
Traffic Control System
Supervisory Computer Control System
Peripheral Devices
Controlling and Monitoring
Traffic Control & Traffic Flow Detection
Video Surveillance and Incident Management

Fig. 2. Smart traffic controlling and monitoring [13].

2|Smart City Overview

A smart city offers a progressive and enhanced lifestyle for the people. A smart city represents a business-oriented and appealing environment. In urban settings, people benefit from different amenities, like PCs, tablets, cell phones, GPS, and sensors.

The estimates for the smart city market are many billion dollars by 2020. This market covers various areas, including smart management, smart movements, smart surveillance, smart transportation [14], smart homes, smart industry, and smart situation handling (*Fig. 3*).

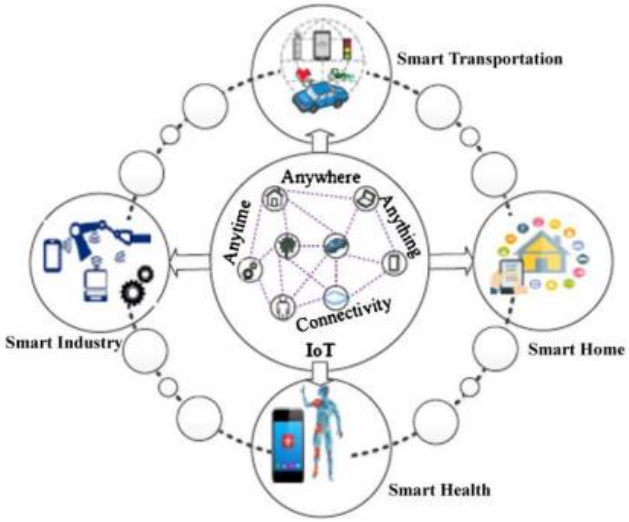

Fig. 3. Application areas of internet of things [15].

2.1 | Key Issues

The key issues of implementing the smart city include:

2.1.1 | Political intervention

Under the political measurement, the essential hindrance is the privacy and decision powers of the distinctive partners.

2.1.2 | Compatibility of heterogeneous innovations

The most pertinent issue concerns the noncompatibility of heterogeneous devices. In this regard, the IoT opens doors for progressive research to examine this problem.

2.1.3 | Monetary issues

Sufficient planning is needed regarding the financial issues. The advantages of smart city concepts are more significant than those of key implementation issues. Some benefits include resource-saving, efficient traffic handling, improved system scalability, and effective city management and planning. *Fig. 4* represents an example of a smart city where the endpoints (People, vehicles, and other things) are connected over the internet.

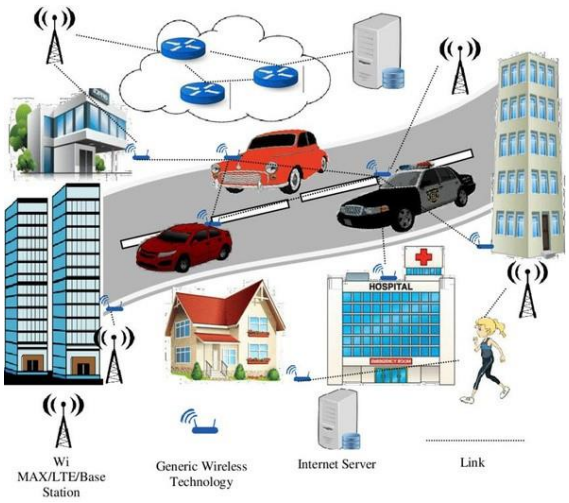

Fig. 4. Example of a smart city.

2.2 | Traffic Handling Schemes in Smart Cities

The main information of ITS includes every one of the components of the vehicle framework, i.e., vehicles, streets, and individuals. Vehicle data relates to checking and viewing vehicle working conditions, including the development condition of the vehicle and its different status characteristics. The data transmission relies upon the corresponding mediums of ITS. It can be separated into wired and wireless systems. Remote transportation of information incorporates FM radio, satellite, and cell phones. For wired transportation of data, optical fiber correspondence has been broadly utilized. The network systems of wired communication also include Wide Area Network (WAN) and Local Area Network (LAN) technologies.

Satellite-based data transportation is broadly utilized in powerful area-based vehicle and routing monitoring. The most well-known cellular systems incorporate GSM, GPRS, and 3G. They have been demonstrated to be powerful and broadly used in ITS-related applications. In ITS, Wi-Fi is predominantly utilized for vehicle sensor systems (VSN), and Wi-Fi passageways are frequently used at the roadside and may accumulate vehicle information by RFID. Many of these technologies are also used in ad hoc networks. Therefore, ad hoc networks can play an important role in implementing traffic monitoring in smart cities [16].

3 | Internet of Things

The IoT would enable clients to oversee and enhance various web devices. A sensor does this procedure to a more prominent degree. They fill in as a connection between the clients and the devices. Sensors gather crude information from ongoing situations and translate it into machine-reasonable organization to effectively exchange it between different "Things." The devices used for deployment of IoT include but are not limited to RFID ,IEEE 802.11, Barcode/QR Code , Zigbee IEEE 802.15.4 and Bluetooth.

3.1 | Problems in Implementing Internet of Things

Some problem areas in implementing IoT technology include:

3.1.1 | Scalability

As IoT technology adapts, billions of devices will be on the internet. Handling such a huge amount will be a real issue.

3.1.2 | Engineering issues

A satisfactory design that grants simple availability, control, correspondences, and valuable applications is important.

3.1.3 | Big data

A tremendous amount of crude information is constantly being gathered. Creating procedures that transform this crude information into usable learning will be important.

3.1.4 | Compatibility

There should be some criteria for handling heterogeneous devices that will communicate with each other.

3.1.5 | Security

Security attacks are a big issue. There is a need to develop rules to handle such issues. Security issues are required to be addressed and designed carefully in the traffic/vehicular system for communication. Many threats exist, such as fake communications initiating traffic disruption or danger compromising the drivers' secretive information. Anonymity might preserve communication in which the vehicle identification/tracking for the non-trusted parties. At an early stage, a lack of privacy rules is considered, which might result in different suitable laws after deploying the network. Each vehicle (Node) contains a permanent unique MAC in the networking field, so it is likely to trace a car with its driver. For this purpose IEEE 802.11p presents

MAC that is assigned dynamically with a duplicate discovery of MAC address. The major goal of IoT is to design an intelligent system based on results collected after analyzing data from the framework. Commonly, messages are controlled and sent from an edge or cloud to actuators/end devices to regulate the physical globe. Therefore, the design of the IoT security is required to compartmentalize the cooperated framework. To attain this, we still need to investigate models of granularity control and the procedures that restrict the proliferation of security breaches.

4 | Ad Hoc Networks

Ad Hoc Networks are self-management networks and are divided into various categories. Some categories include (*Fig. 5*):

I. Mobile Ad Hoc Networks (MANETs)

II. Vehicular Ad Hoc Networks (VANETs)

III. Wireless Sensor Networks (WSNs)

IV. RFID

The challenges and issues of different types of ad hoc networks are discussed below. A brief overview of these categories and their connection strategies with IoT is also provided.

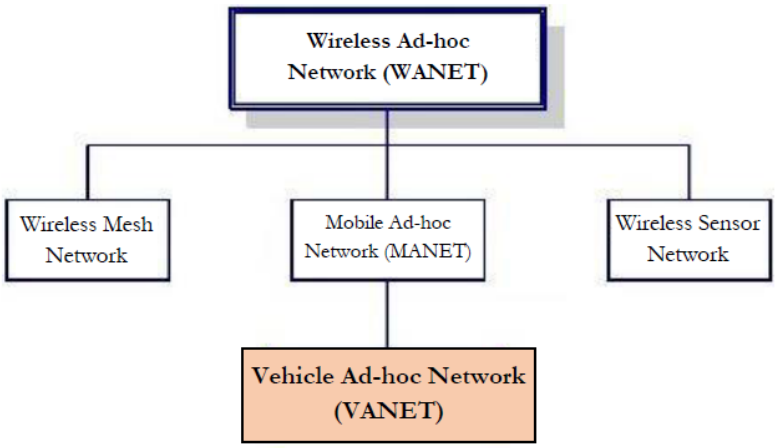

Fig. 5. Hierarchy of wireless Ad hoc networks [17].

4.1 | Mobile Ad Hoc Networks

MANETs face several significant challenges due to their dynamic and decentralized nature. One of the primary issues is the dynamic topology, as the frequent movement of nodes leads to constant changes in the network structure, complicating the maintenance of stable routes. This mobility also affects routing protocols, which must quickly adapt to changes, often resulting in increased latency and route failures. Limited bandwidth in wireless links can cause congestion and reduce throughput, while energy constraints are a concern since many mobile devices rely on battery power, necessitating energy-efficient communication protocols [18].

4.2 | Vehicular Ad Hoc Networks

VANETs encounter various challenges due to their unique environment and requirements. One major challenge is the high mobility of vehicles, which can lead to rapidly changing network topologies, making it

difficult to establish and maintain stable communication links. This dynamic environment also complicates the design of effective routing protocols, as vehicles may move in and out of range quickly [19].

4.3 | Wireless Sensor Networks

WSNs [20] face several challenges that stem from their unique characteristics and operational environments. One primary challenge is energy management, as sensor nodes are typically battery-powered and must operate efficiently to prolong their lifespan. This necessitates energy-efficient communication protocols and algorithms.

Another significant challenge is scalability. As the number of sensor nodes increases, the network must effectively handle larger data volumes and maintain performance without degradation. The dynamic nature of the environment can also impact network reliability, as nodes may fail or be removed, leading to the need for robust self-healing capabilities.

Data management presents additional hurdles, particularly in ensuring the accurate collection, processing, and transmission of data. The limited wireless communication bandwidth can result in congestion, primarily when multiple nodes transmit data simultaneously.

4.4 | Radio-Frequency Identification

RFID technology faces several significant challenges that can impact its effectiveness and implementation [9]. One major issue is interference and signal blockage, as other electronic devices or physical barriers, such as metal objects or liquids, can disrupt RFID systems, which hinder communication between tags and readers. Security and privacy are also critical concerns; RFID systems are vulnerable to threats like eavesdropping, tag cloning, and unauthorized access, necessitating robust measures to ensure data integrity and protect user privacy.

Another challenge is tag collision, where multiple tags within a reader's range can interfere with each other, leading to data loss or miscommunication; effective anti-collision algorithms are essential to manage this.

5 | Interfacing Ad Hoc Networks to Internet of Things

5.1 | Interfacing Mobile Ad Hoc Networks to Internet of Things

A few methodologies have been presented to interface MANETs systems to the internet.

The hubs in MANETs use Internet Protocol (IP) addresses for directing purposes; such IPs might be utilized to move information over the internet. In any case, the principle issue of this methodology is that a hub needs a productive method to check whether a specific IP in the MANET is available. On a fundamental level, hubs don't know about their specific situations, so it is hard to gather neighboring hubs IPs.

One methodology is to utilize two unique IPs, one to transmit through the internet and another to recognize hubs in the MANET. In such a case, hubs can move openly, so the objective passage could be variable. If a hub changes to another entryway, another IP address ought to be utilized, and the active associations will most likely break.

Then again, the expanding utilization of smart cell phones empowers hubs to associate with the internet through cellular devices, such as 3G and 4G advances. Additionally, satellite correspondence can be utilized in safety-related applications like military applications and traffic congestion.

5.2 | Interfacing Vehicular Ad Hoc Networks to Internet of Things

Interfacing VANETs with IoT is like the methods utilized in MANETs. Therefore, vehicular systems are typically associated with the internet by methods for APs utilizing Wireless Local Area Networks (WLAN), such as WiFi, WiMAX, or Bluetooth.

5.3 | Interfacing Wireless Sensor Networks with Internet of Things

To interface basic gadgets of WSNs with the IoT, three models can be characterized: 1) the IP overlay over WSN, 2) the sensor overlay over IP, and 3) the more elevated amount of entryway overlays. When IP overlays over WSN, sensor hubs should have IPs similar to those associated with the Web. In the second model, information is typified in IP data, which the portal interprets directly.

5.4 | Interfacing Radio-Frequency Identification to Internet of Things

The RFID Tags can easily be associated with the IoT. RFID readers gather data from Tags and redirect data to the internet. RFID readers are used as interpreters of RFID data and internet-based data.

6 | Literature Study on Intelligent Traffic Systems Using Ad Hoc Networks or Internet of Things for Smart Cities

The above study reflects the introduction of IoT, ad hoc networks, smart cities, and techniques to interconnect them. The combined work on all these technologies at a time in a traffic congestion scenario is very rarely found.

However, the literature regarding the combination of two or more technologies is presented in this section. This will help the readers to have future directions to work in the area of traffic congestion related to the abovementioned technologies all at a time or a part of them. The work uses GPS and guiding data from the city, which has the correct location of the International Territorial Level (ITLs). This helps the vehicles to find the closest ITL. Every vehicle sends a request message after some interval to get the correct area of each vehicle. This enables us to understand the traffic density. The work depicts a social network of vehicles by clustering the vehicles on a characteristic basis.

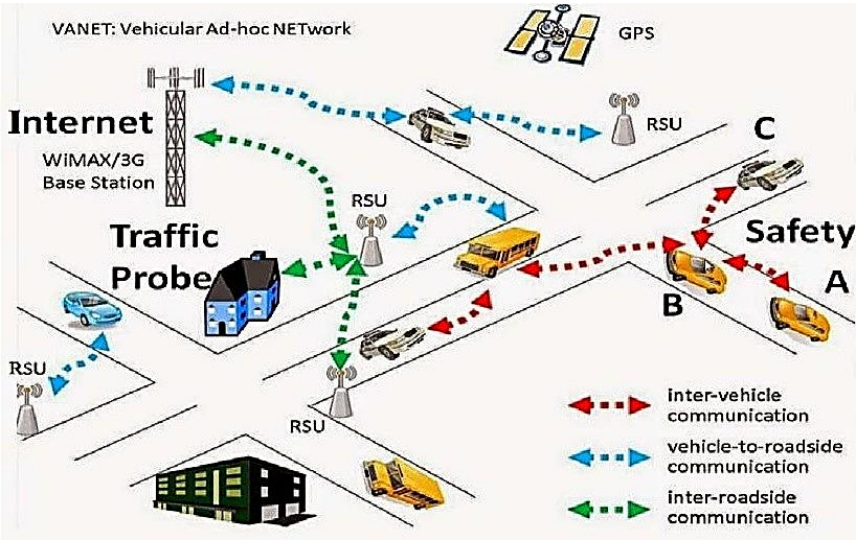

Fig. 6. Clustering of vehicles in ad hoc networks.

7 | Conclusion

This manuscript highlights the different technologies that can help manage traffic in smart cities. The core technologies considered include IoT and ad hoc networks. An overview of these technologies is presented, along with the issues and devices used for communication. It is observed that various devices in IoT and ad hoc work can be used to make a hybrid network for traffic congestion management systems in smart cities. In addition, a brief survey of some intelligent transportation approaches is also presented.

In conclusion, integrating Autonomous Vehicle (AV) networking within smart cities through the IoT represents a significant advancement in urban mobility and infrastructure management. This interconnected ecosystem can enhance traffic efficiency, reduce congestion, and improve safety by enabling real-time communication between vehicles, infrastructure, and various urban services. The potential benefits include reduced emissions, streamlined public transport, and improved emergency response times.

However, realizing this vision is contingent upon addressing key challenges, such as ensuring cybersecurity, protecting user privacy, and developing standardized protocols for interoperability. Effective collaboration among policymakers, technology developers, and urban planners is essential to create a regulatory framework that supports innovation while safeguarding public interests.

As smart cities continue to evolve, leveraging IoT for AV networking offers a pathway to more sustainable, efficient, and resilient urban environments. Future research and development efforts should focus on overcoming existing barriers, exploring advanced technologies, and fostering interdisciplinary partnerships to maximize the societal benefits of this transformative approach to urban mobility.

Funding

This research received no external funding.

Data Availability

The data used and analyzed during the current study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The author declare no conflicts of interest regarding the publication of this paper.

If necessary, these sections should be tailored to reflect the specific details and contributions.

References

[1] Al-Turjman, F., & Lemayian, J. P. (2020). Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: An overview. *Computers & electrical engineering*, *87*, 106776. https://doi.org/10.1016/j.compeleceng.2020.106776

[2] Hegarty, C. J. (2017). The global positioning system (GPS). In *Springer handbook of global navigation satellite systems* (pp. 197–218). Cham: Springer, Cham. https://doi.org/10.1007/978-3-319-42928-1_7

[3] Baby Shalini, V. (2022). Global positioning system (GPS) and internet of things (IoT) based vehicle tracking system. *Inventive computation and information technologies* (pp. 481–492). Singapore: Springer, Singapore. https://doi.org/10.1007/978-981-16-6723-7_36

[4] Wilde, E. (1999). Hypertext transfer protocol (HTTP). In *World wide web: Technische grundlagen* (pp. 53–149). Berlin, Heidelberg: Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-59944-6_4

[5] Young, S., & Aitel, D. (2003). Simple mail transfer protocol (SMTP). In *The hacker's handbook* (pp. 411–462). Auerbach Publications. https://doi.org/10.1201/9780203490044

[6] Wright, L. (2000). Wireless application protocol (WAP). *Interactive marketing*, *2*(2), 148–157. https://doi.org/10.1057/palgrave.im.4340083

[7] Novack, D. (2008). Next generation telematics protocol. *15th world congress on intelligent transport systems and its America's 2008 annual meetingits americaerticoits japantranscore*. TRB. https://trid.trb.org/View/904260

[8] Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. *Future generation computer systems*, *79*, 849–861. https://doi.org/10.1016/j.future.2017.09.020

[9] Roberts, C. M. (2006). Radio frequency identification (RFID). *Computers & security*, *25*(1), 18–26. https://doi.org/10.1016/j.cose.2005.12.003

[10] Parida, B. R., Rath, A. K., & Mohapatra, H. (2022). Binary self-adaptive salp swarm optimization-based dynamic load balancing in cloud computing. *International journal of information technology and web engineering (IJITWE)*, *17*(1), 1-25. https://doi.org/ 10.4018/IJITWE.295964

[11] Bitam, S., & Mellouk, A. (2012). ITS-cloud: Cloud computing for intelligent transportation system. *2012 IEEE global communications conference (GLOBECOM)* (pp. 2054–2059). IEEE. https://doi.org/10.1109/GLOCOM.2012.6503418

[12] Winston, C. (2013). On the performance of the US transportation system: Caution ahead. *Journal of economic literature*, *51*(3), 773–824. http://dx.doi.org/10.1257/jel.51.3.773

[13] Rath, M. (2018). Smart traffic management system for traffic control using automated mechanical and electronic devices. *Institute of physics conference series: Materials science and engineering* (pp. 12201). Institute of physics publishing. https://dx.doi.org/ 10.1088/1757-899X/377/1/012201

[14] Mohapatra, H., Rath, A. K., & Panda, N. (2022). IoT infrastructure for the accident avoidance: An approach of smart transportation. *International Journal of Information Technology*, *14*(2), 761-768. https://doi.org/10.1007/s41870-022-00872-6

[15] Xu, Y. (2023). Routing strategies and protocols for efficient data transmission in the internet of vehicles: A comprehensive review. *International journal of advanced computer science and applications*, *14*(9), 955–965. https://doi.org/10.14569/IJACSA.2023.01409100

[16] Cunha, B., Brito, C., Araújo, G., Sousa, R., Soares, A., & Silva, F. A. (2021). Smart traffic control in vehicle ad-hoc networks: A systematic literature review. *International journal of wireless information networks*, *28*(3), 362–384. https://doi.org/10.1007/s10776-021-00517-8

[17] LA, V. (2014). Security attacks and solutions in vehicular ad hoc networks: A survey. *International journal on adhoc networking systems (IJANS)*, *4*, 1–20. http://dx.doi.org/10.5121/ijans.2014.4201

[18] Bang, A. O., & Ramteke, P. L. (2013). MANET: History, challenges and applications. *International journal of application or innovation in engineering & management (IJAIEM)*, *2*(9), 249–251. https://www.researchgate.net/publication/331653159

[19] Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2017). VANet security challenges and solutions: A survey. *Vehicular communications*, *7*, 7–20. https://doi.org/10.1016/j.vehcom.2017.01.002

[20] Raghavendra, C. S., Sivalingam, K. M., & Znati, T. (2006). *Wireless sensor networks*. Springer. https://doi.org/10.1007/b117506